Konfiguration der ICMP-Filterung (Internet Control Message Protocol) auf den Managed Switches der Serie 300

Ziel

Internet Control Message Protocol (ICMP) ist ein Protokoll auf Netzwerkebene, das zur Meldung und Benachrichtigung von Fehlern und zur Netzwerkerkennung verwendet wird. In einem Netzwerk mit ICMP können viele Angriffe durchgeführt werden. Ein ICMP-Flood-Denial-of-Service-Angriff (DoS) ist beispielsweise ein Angriff, der Sicherheitslücken im ICMP-Protokoll und eine falsche Netzwerkkonfiguration ausnutzt. Die ICMP-Filterung ist eine Lösung zur Verhinderung dieser Art von Angriffen auf das Netzwerk. Sie können den Switch so konfigurieren, dass die IP-Adressen oder Ports gefiltert werden, von denen Sie ICMP-Pakete blockieren möchten. In diesem Artikel wird die Konfiguration der ICMP-Filterung für die Managed Switches der Serie 300 erläutert.

Anwendbare Geräte

·Managed Switches der Serie SF/SG 300

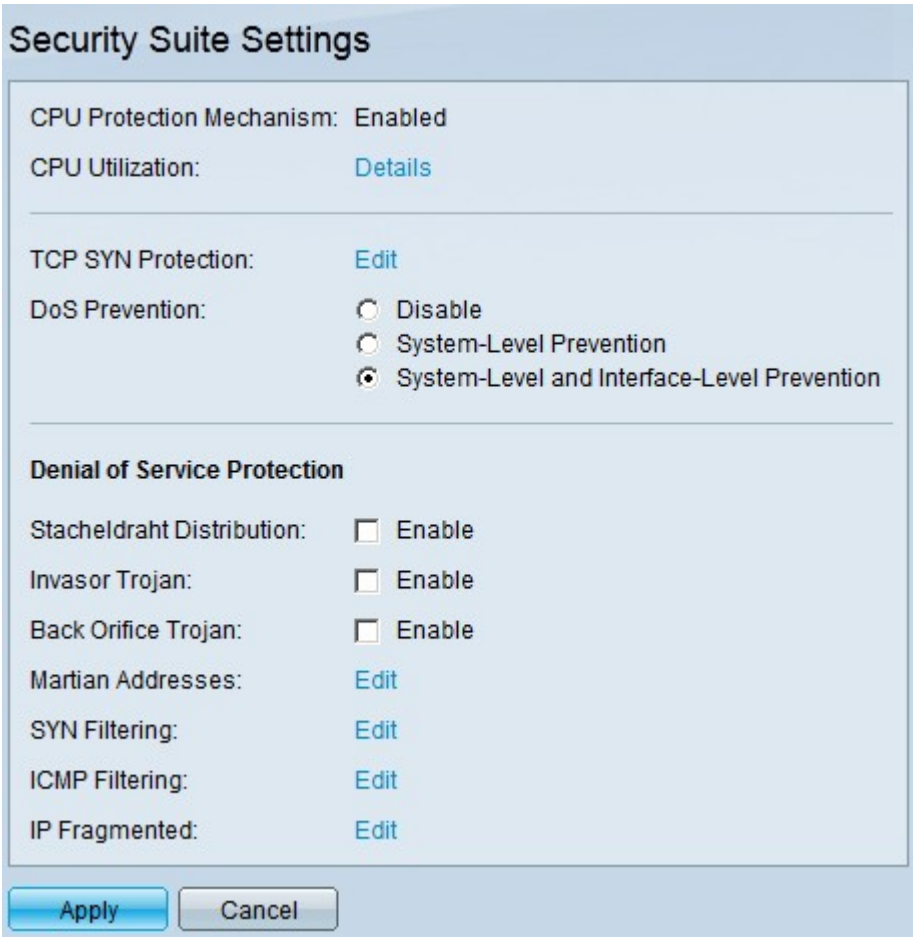
Softwareversion

·1.3.0.62

Denial of Service Level Prevention aktivieren

Um die ICMP-Filterung anwenden zu können, müssen Sie zunächst sicherstellen, dass der Switch die richtige Einstellung zur Vermeidung von 'Denial of Service'-Levels aufweist. In diesem Abschnitt wird erläutert, wie Sie die richtige Präventionsstufe für die Managed Switches der Serie 300 aktivieren.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Denial of Service Prevention > Security Suite Settings aus**. Die Seite *SicherheitsSuite-Einstellungen* wird geöffnet:



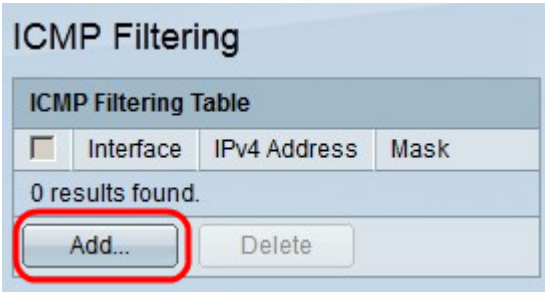
Schritt 2: Im Bereich *DoS-Prävention* gibt es drei Präventionsstufen. Klicken Sie auf das Optionsfeld **Schutz auf Systemebene und Schnittstellenebene**. Auf dieser Ebene können Sie die ICMP-Filterung konfigurieren.

Schritt 3: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

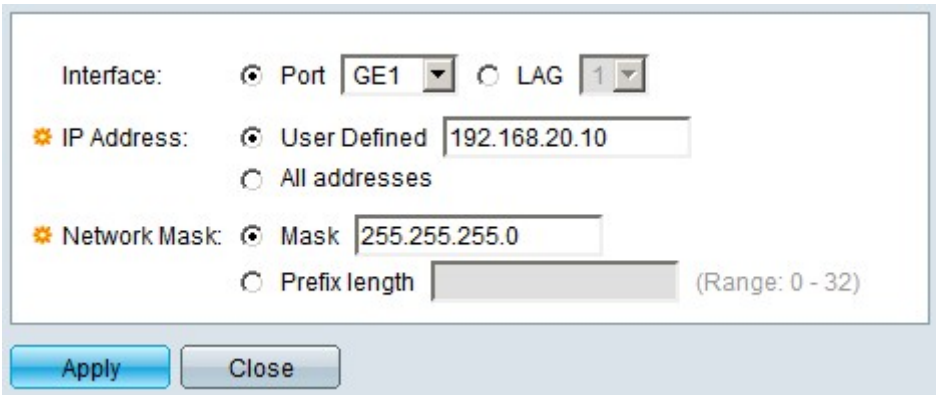
ICMP-Filterkonfiguration

In diesem Abschnitt wird die Konfiguration der ICMP-Filterung für die Managed Switches der Serie 300 erläutert.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Denial of Service Prevention > ICMP Filtering aus**. Die Seite *ICMP-Filterung* wird geöffnet:



Schritt 2. Klicken Sie auf **Hinzufügen**. Das Fenster *ICMP-Filterung hinzufügen* wird angezeigt.



Schritt 3: Klicken Sie im Feld *Schnittstelle* auf das Optionsfeld einer der verfügbaren Schnittstellenoptionen:

·Port - Ermöglicht Ihnen die Auswahl des Ports, von dem Sie ICMP-Pakete filtern möchten.

·LAG: Hier können Sie die LAG auswählen, von der Sie ICMP-Pakete filtern möchten. Die LAG fasst mehrere Ports zu einem logischen Port zusammen.

Schritt 4: Klicken Sie im Feld *IP-Adresse* auf das Optionsfeld einer der verfügbaren Optionen, um die IP-Adresse(n) zu definieren, aus der/denen ICMP-Pakete gefiltert werden sollen aus:

·Benutzerdefiniert - Benutzerdefinierte ICMP-Paketquellen.

·Alle Adressen - Alle IP-Adressen-ICMP-Paketquellen.

Schritt 5 Klicken Sie im Feld *Network Mask (Netzwerkmaske*) auf das Optionsfeld einer der verfügbaren Optionen, um die Netzwerkmaske der in Schritt 4 konfigurierten IP-Adresse einzugeben:

·Maske - Subnetzmaske im Punktformat, z. B. 255.255.255.0.

·Präfixlänge - Subnetzmaske im Schrägstrich-Format, z. B. \24.

Schritt 6: Klicken Sie auf **Apply**, um die Konfiguration zu speichern.

Das nachfolgende Bild zeigt die Änderungen nach der Konfiguration:

Schritt 7: (Optional) Um einen ICMP-Filter zu löschen, aktivieren Sie das Kontrollkästchen des ICMP-Filters, den Sie in der ICMP-Filtertabelle löschen möchten, und klicken Sie dann auf **Löschen**.